REMARKS

Claims 1-28, 30, 31, and 33-41 are pending in this application, all of which have been finally rejected as a result of the January 27, 2005 Office Action. For the reasons set forth below, applicants believe that the rejection is not sustainable on the grounds proffered. Thus, applicants respectfully request that the Examiner reconsider and withdraw the final rejection, and allow this case.

The claims have been rejected as being unpatentable over U.S. Patent No. 5,689,565 (Spies) in view of U.S. Patent No. 6,385,727 (Cassagnol). The claims of the present application relate generally to cryptography, and Spies generally describes a system that applies cryptographic keys to data. The independent claims of the present case – while different from each other in both scope and language – recite various features relating to the unavailability of certain cryptographic keys under certain circumstances. As to these unavailability features, the Examiner has not set forth any argument that these features are taught, suggested, or motivated by Spies, but rather has applied Cassagnol to these features. Thus, the issue in this case is whether Cassagnol teaches the unavailability features.[1]

Cassagnol is generally directed to cryptography. Principally, Cassagnol describes a system in which cryptographic keys are protected from divulgence by storing them in an EEPROM, securely delivering the keys to a "crypto" module, and physically protecting the EEPROM and the path to the crypto module in order to prevent divulgence of the keys. (Cassagnol, col. 17, ll. 1-15.) The premise of Cassagnol is that the keys can be stored in the EEPROM and transmitted through a channel to the crypto module, because the EEPROM, crypto module, and channel between them are protected so as to prevent the keys from being intercepted. In other words, Cassagnol makes the keys available to the module that will perform cryptographic operations under physically controlled circumstances, but uses various protection means to prevent the keys from being intercepted.

[1] It should be understood that applicants' referring to various features in the independent claims as the "unavailability features" is not intended to imply that these features are in any way co-extensive in scope or meaning. The claims have differing scope, which is apparent from the claims' actual text. Applicants have simply used the term "unavailability features" for the Examiner's convenience grouping together and analyzing a set of claim features that are related but not the same.

By contrast, the claimed invention protects cryptographic keys by causing them to meet certain standards of unavailability with respect to the software that will actually apply the key. In particular, these features, as recited in claims 1, 9, 20, 25, and 31 are as follows:

- Claim 1 recites a secure repository that "comprises a software module that uses a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being stored in a memory accessible to said [secure repository]"

- Claim 9 recites a secure repository that "comprises a software module that uses a cryptographic algorithm to apply a cryptographic key to data without said cryptographic key being stored in a memory."

- Claim 20 recites a secure repository that comprises computer-executable instructions that apply a cryptographic key "without said cryptographic key being stored in any memory during the time that [the] computer-executable instructions appl[y] said cryptographic key."

- Claim 25 recites a method that uses a secure repository to apply a cryptographic key "without said cryptographic key being stored in a memory."

- Claim 31 recites a method that uses a software process that applies a cryptographic key "without said cryptographic key being stored in a memory usable by said ... software process during a time that [the] software process is applying said cryptographic key."

Cassagnol does not teach or suggest any of these features, since Cassagnol does not rely on keys not being stored in a memory but rather on protection of the memory that does store the keys. As noted in applicants' September 23, 2004 paper and for the reasons described therein, Cassagnol teaches away from claims 1, 20, and 31, since these claims call for the key to be inaccessible to the secure repository that is applying the key (claim 1), or not stored in any memory during the time the key is being applied (claim 20), or not stored in a memory that is usable by the software process applying the key at the time the key is being applied (claim 31). These features are wholly incompatible with Cassagnol, since Cassagnol teaches that the crypto module uses and applies the keys that are stored in the EEPROM.

In the January 27, 2005 Office Action, the Examiner does not appear to dispute this distinction between the present claims and Cassagnol, and acknowledges that Cassognol's approach is "somewhat different." However, the Examiner maintains the rejection of the

claims on the ground that the claims and Cassagnol are "functionally similar." Applicants respectfully submit that "functionally similar" is not the relevant standard under which to determine obviousness under 35 U.S.C. § 103(a).

First, it should be noted that, with the Examiner having acknowledged that Cassagnol takes a "somewhat different" approach from the claimed invention, the Examiner has effectively taken the obviousness rejection out of the realm of "combination" and placed it into the realm of "modification." Modification of a reference is permissible in an obviousness rejection, provided that the prior art provides some motivation to modify the reference in the manner proposed. See MPEP 2143.01. The various rationales that are recognized as motivating a proposed combination or modification are set forth in MPEP 2144, and functional similarity is not regarded as sufficient reason to support an obviousness rejection. Specifically, MPEP 2144.06 states:

> In order to rely on equivalence as a rationale supporting an obviousness rejection, the equivalency must be recognized in the prior art, and *cannot be based on* applicant's disclosure or *the mere fact that the components at issue are functional or mechanical equivalents*.

[Emphasis added.] Thus, the Examiner's basis to maintain the rejection of the claims is contrary to the MPEP.

In substance, what the Examiner has found is that Cassagnol and the present application are directed to two different mechanisms for protecting keys. Even if this is so, it is not generally the case that any two mechanisms that accomplish the same purpose are patentable indistinct from each other. Rather, in order to establish obviousness, it must be shown why the prior art would motivate one to do what is claimed. The present Office Action fails to establish such motivation. It is unclear why one would read Cassagnol – with its teachings about storing keys in memory's that are protected from observation – and be motivated to practice the present invention, where keys are protected by not storing them in certain memories. Nor is it clear how someone would read Cassagnol and be motivated to have keys applied by software to which those keys are inaccessible (as in claims 1, 20, and 31), since Cassagnol does not explain how does not explain how keys that are inaccessible can be applied. (The present application does explain example relevant techniques at pages 47-51).

For these reasons, applicants respectfully submit that the obviousness rejection is not sustainable, and is grounded in a rationale that is not consistent with the standards for obviousness as set forth in the MPEP.

Conclusion

For the foregoing reasons, independent claims 1, 9, 20, 25, and 31 have been shown to be patentable over the applied prior art, and claims 2-8, 10-19, 21-24, 26-29, and 33-41 are patentable at least by reason of their dependency. Applicants thus respectfully request that the Examiner reconsider and withdraw the final rejection of all pending claims, and issue a Notice of Allowance in the next Office Action.

Date: March 25, 2005

Sharon Fenick
Registration No. 45,269

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439